الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Référentiel d'audit de la sécurité des systèmes d'information

26/10/2018

Cadre de référence de l’audit

- Loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique et portant sur l'organisation du domaine de la sécurité informatique et fixant les règles générales de protection des systèmes informatiques et des réseaux,
- Décret n° 2004-1250 du 25 mai 2004, fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit,
- Décret n° 2004-1249 du 25 mai 2004, fixant les conditions et les procédures de certification des experts auditeurs dans le domaine de la sécurité informatique.

Cadre de référence de l'audit

Les décrets sus-cités n'identifient pas les contrôles de sécurité à vérifier

l'ANSI estime qu'il est nécessaire d'identifier les critères d'audit à travers un document de référentiel qui permettra:

- d'accompagner les experts auditeurs dans la réalisation des missions d'audit de sécurité des systèmes d'information,
- aux organismes audités de disposer de garanties sur la qualité des audits effectués
- et aux services de suivi de l'audit au sein de l'ANSI de mener efficacement l'étude et l'évaluation des rapports d'audit.

Références

- La norme ISO 19011 :2011, Lignes directrices pour l’audit des systèmes de management,
- La norme ISO 27001 :2013, Systèmes de management de la sécurité de l’information,
- La norme ISO 27002 :2013, Code de bonnes pratiques pour le management de la sécurité de l'information.

Documents requis pour la revue

- L'ensemble des politiques de sécurité de l'information de l'audité, approuvées par la direction,
- Le manuel de procédures relatif à la sécurité de l'information:
  - La procédure de mise à jour des documents de politiques de sécurité et des procédures,
  - La procédure d'attribution des responsabilités,
  - La procédure de classification des actifs,
  - procédure de gestion des incidents,
  - Les procédures de gestion de la continuité des activités,
  - Etc …
- Les fiches de poste du RSSI et des autres employés en relation avec la sécurité du système d'Information,
- La matrice de flux des données,
- Les schémas d'architecture du système d'information,
- L'inventaire du matériel et logiciel informatique,
- Etc …

Echantillonnage

Les critères d'échantillonnage pour chaque type de composante du système d'information à auditer doivent être bien définis et justifiés.

Types de vérification

Les vérifications à effectuer tout au long de la mission d'audit sont de type organisationnel, physique ou technique présentés par la légende suivante :

Type	Couleur
Organisationnel	
Physique	
Technique	

Contenu

Réf Annexe A (ISO 27001)	Titre Domaine/Objectif/Contrôle	Description	Vérifications à effectuer	Moyen de vérification (sans s'y limiter)	Preuves
A.5	**Politiques de sécurité de l'information**				
A.5.1	Orientations de la direction en matière de sécurité de l'information	Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.			
A.5.1.1	Politiques de sécurité de l'information	Un ensemble de politiques de sécurité de l'information (PSI) doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.	• S'il existe des documents de politiques de sécurité de l'information, qui sont approuvées par la direction, publiées et communiquées, à tous les utilisateurs du SI et aux tiers concernés	• Revue des documents de PSI, • Entretien avec le DG, • Interviews d'un échantillon des utilisateurs, • Revue des PVs de réunion du comité de sécurité	• Documents de PSI approuvées par la DG, • Echantillon de décharges (ou courriers électroniques) attestant que les utilisateurs ont reçu une copie des PSI, • Historique des mises à jour des PSI, • PV de réunion du comité de sécurité sur la màj de la PSI, • procédures en place pour le réexamen des PSI.
A.5.1.2	Revue des politiques de sécurité de l'information	Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.	• Si ces politiques sont passées en revue par un comité de sécurité de haut niveau à intervalles planifiés, ou si des changements importants se produisent pour s'assurer qu'elles sont toujours pertinentes, adéquates et efficaces, • S'il existe des procédures en place pour le réexamen des politiques de sécurité de l'information		

Contenu

A.6	**Organisation de la sécurité de l'information**				
A.6.1	Organisation interne	Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisme.			
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.	• Si un RSI, doté d'un pouvoir décisionnel et assurant le reporting directement à la direction, est désigné, • Si un comité de sécurité est mis en place, • Si les rôles et les responsabilités liés à la sécurité de l'information sont bien définis et attribués à des individus ayant les compétences requises.	Revue de l'organigramme, des fiches de poste, des décisions et notes internes en relation avec la sécurité du SI, Entretien avec le DG, Interview du RSI (le cas échéant).	Décision de nomination du RSI, Décision de mise en place du comité de sécurité, PVs de réunions du comité, Fiches de poste.
A.6.1.2	Séparation des tâches	Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisme.	• Si les tâches incompatibles Sont identifiées et les responsabilités sont attribuées en conséquence, • Si une tâche de vérification régulière, de la définition et de l'attribution des responsabilités, est prévue et réalisée, • Si des contrôles compensatoires sont mis en place en cas d'attribution des tâches incompatibles à la même personne.	Revue des fiches de poste, Entretien avec les responsables des services métier pour l'identification des taches incompatibles, Revue des procédures internes qui identifient les tâches incompatibles, Vérification des droits d'accès sur les systèmes qui hébergent ou traitent les services concernés, Vérification des contrôles compensatoires en cas en cas d'attribution des tâches incompatibles à la même personne.	Fiches de poste, Compte rendu de vérification de la définition et de l'attribution des responsabilités.

Contenu

A.7	Sécurité des ressources humaines				
A.7.1	Avant l'embauche	S'assurer que les salariés et les sous-traitants comprennent leurs responsabilités et sont qualifiés pour les rôles qu'on envisage de leur donner.			
A.7.1.1	Sélection des candidats	Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	• Si des contrôles de vérification de fond pour tous les candidats à l'emploi ont été réalisés conformément à la réglementation en vigueur, • Si la vérification comprend le certificat de moralité, la confirmation des qualifications académiques et professionnelles prétendues et des contrôles indépendants d'identité, • Si un candidat pour un poste spécifique de sécurité de l'information possède les compétences nécessaires pour ce poste et s'il est digne de confiance surtout si le poste est critique pour l'organisme	Revue du statut et du règlement intérieur, Revue de la procédure de recrutement, Revue du dossier du RSI et d'un échantillon de personnes impliqués dans la sécurité, Interview du DRH.	Statut et règlement intérieur, fiches de postes des personnes impliquées directement dans la sécurité de l'information, Procédure de recrutement Dossier du RSI et des personnes impliquées dans la sécurité de l'information.
A.7.1.2	Termes et conditions d'embauche	Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisme en matière de sécurité de l'information.	• Si les employés et les sous-traitants sont invités à signer un engagement de confidentialité ou de non-divulgation dans le cadre de leurs termes et conditions initiaux du contrat de travail, • Si cet engagement de confidentialité couvre la responsabilité de l'audité et des employés et des sous-traitants concernant la sécurité de l'information.	Revue d'un échantillon des engagements de confidentialité, Interview du DRH et du DAF.	Echantillon des Engagements de confidentialité signés par les employés et les sous-traitants.
A.7.2	Pendant la durée du contrat	S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.			
A.7.2.1	Responsabilités de la direction	La direction doit demander à tous les salariés et sous-traitants d'appliquer les règles de sécurité de l'information	• Si la direction exige explicitement (par une note interne signée par le DG) que les employés et les sous-traitants appliquent les	Revue de la note interne signée par le DG, Revue d'un échantillon de contrats avec les sous-traitants,	Note interne signée par le DG, Echantillon de contrats avec les sous-traitants

Contenu

A.8	Gestion des actifs				
A.8.1	Responsabilités relatives aux actifs	Identifier les actifs de l'organisme et définir les responsabilités pour une protection appropriée.			
A.8.1.1	Inventaire des actifs	Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.	• S'il existe des règles relatives à l'inventoring des actifs au niveau de la PSI, qui exigent le maintien d'un inventaire des actifs, • Si des procédures d'inventoring des actifs sont développées et maintenues, • Si un inventaire ou registre est maintenu pour tous les actifs de l'audité.	Revue de la PSI pour l'identification des règles relatives à l'inventoring, Revue des procédures d'inventoring des actifs, Revue de l'inventaire et vérification de son exhaustivité, Interview du DAF, Interview du DSI.	PSI, Procédures d'inventoring, Inventaire des actifs.
A.8.1.2	Propriété des actifs	Les actifs figurant à l'inventaire doivent être attribués à un propriétaire.	• Si chaque actif identifié a un propriétaire	Revue de l'inventaire et vérification de l'existence du nom du propriétaire de chaque actif.	Inventaire des actifs.
A.8.1.3	Utilisation correcte des actifs	Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.	• Si une politique d'utilisation correcte de l'information, des actifs associés et des moyens de son traitement est élaborée et mise en œuvre, • Si les employés et les sous-traitants ont été sensibilisés aux exigences de sécurité comprises dans cette politique et de leur responsabilité de l'utilisation de ces actifs.	Revue de la politique d'utilisation correcte de l'information, Revue d'un échantillon de contrats avec les sous-traitants ayant l'accès aux moyens de traitement de l'information, Interview du RSI et du DSI, Interview du DRH et du DAF.	Politique d'utilisation correcte de l'information, Echantillon de contrats avec les sous-traitants ayant l'accès aux moyens de traitement de l'information.

Contenu

A.9	Contrôle d'accès				
A.9.2	Gestion de l'accès utilisateur	Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.			
A.9.2.1	Enregistrement et désinscription des utilisateurs	Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.	• Si un processus d'enregistrement et de désinscription des utilisateurs, qui définit les étapes à suivre pour ajouter un utilisateur et pour supprimer un utilisateur suite à la fin de son travail, est défini et mis en œuvre, • Si des identifiants utilisateur uniques sont utilisés pour tenir les utilisateurs responsables de leurs actions, • Si l'utilisation d'identifiants partagés n'est autorisée que lorsqu'elle est nécessaire pour des raisons commerciales ou opérationnelles et si elle est approuvée et documentée, • Si les identifiants utilisateur redondants sont périodiquement identifiés et supprimés ou désactivés.	Revue du processus d'enregistrement et de désinscription des utilisateurs, Interview de l'administrateur systèmes, BD et réseaux, Vérification des comptes utilisateurs sur les serveurs pour l'identification de ceux qui sont partagés, redondants ou obsolètes.	Document du processus d'enregistrement et de désinscription des utilisateurs, Liste des comptes utilisateurs sur les serveurs.

Contenu

A.10	**Cryptographie**				
A.10.1	Mesures cryptographiques	Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.			
A.10.1.1	Politique d'utilisation des mesures cryptographiques	Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.	• Si une politique d'utilisation des mesures cryptographiques est élaborée et mise en œuvre, • Si la direction adopte une approche en ce qui concerne l'utilisation de mesures cryptographiques pour la protection de l'information liée à l'activité de l'organisme, • Si le niveau de protection requis, en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement requis, est identifié sur la base d'une appréciation du risque, • Si les liens permanents et les échanges de données devant être protégés par des solutions de chiffrement sont définis et si ces solutions sont mises en place au niveau du réseau local et du réseau étendu, • Si les transactions sensibles devant être protégés par des solutions de chiffrement sont définies et si ces solutions sont mises en place au niveau applicatif.	Revue de la politique d'utilisation des mesures cryptographiques, Revue de rapport d'analyse des risques, Entrevue avec le DG, Interview des administrateurs systèmes, réseaux, BD et applications, Test des solutions de chiffrement mises en place au niveau des serveurs, des équipements réseaux et de sécurité et des applications.	Politique d'utilisation des mesures cryptographiques, Rapport d'analyse des risques, Rapports de test des solutions de chiffrement.

Contenu

A.11	**Sécurité physique et environnementale**				
A.11.1	Zones sécurisées	Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisme.			
A.11.1.1	Périmètre de sécurité physique	Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.	• Si les périmètres de sécurité sont définis et si l'emplacement et le niveau de résistance de chacun des périmètres sont fonction des exigences relatives à la sécurité des actifs situés à l'intérieur et des conclusions de l'appréciation du risque, • Si le périmètre d'un bâtiment ou d'un site abritant des moyens de traitement de l'information est physiquement solide (le périmètre ou les zones ne présentent aucune faille susceptible de faciliter une intrusion), • Si le toit, les murs extérieurs et le sol du site sont construits de manière solide et si les portes extérieures sont toutes convenablement protégées contre les accès non autorisés par des mécanismes de contrôle, par exemple des barres, des alarmes, des verrous, • Si les portes et les fenêtres non gardées sont verrouillées, et si une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée, est en place, • Si un personnel à l'accueil ou des moyens de contrôle d'accès physique au site ou au bâtiment sont placés, • Si l'accès aux sites et aux bâtiments est limité aux seules personnes autorisées,	Revue du rapport d'analyse des risques, Revue du plan d'architecture du bâtiment de l'audité et identification des périmètres de sécurité physique, Revue du rapport de test des mécanismes de sécurité contre les dommages d'intrusion physiques, d'incendies, d'inondations, de perturbation des services généraux Interview du DAF, du responsable de la sécurité physique et du RSI, Inspection visuelle des périmètres de sécurité.	Rapport d'analyse des risques, Plan d'architecture du bâtiment de l'audité, Rapport de test des mécanismes de sécurité, Photos.

Contenu

A.12	**Sécurité liée à l'exploitation**				
A.12.1	Procédures et responsabilités liées à l'exploitation	Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.			
A.12.1.1	Procédures d'exploitation documentées	Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.	• Si les procédures opérationnelles d'exploitation (systèmes, applications, BD, équipements et solutions réseau et sécurité, etc.) sont documentées, • Si la documentation des procédures opérationnelles d'exploitation est maintenue à jour, • Si les modifications des procédures d'exploitation sont approuvées par les responsables concernés, • Si les procédures opérationnelles d'exploitation sont rendues disponibles à toute personne en ayant besoin, • Si ces procédures sont protégées contre des altérations illicites, • Si l'authenticité et la pertinence des procédures opérationnelles font l'objet d'un audit régulier.	• Revue des procédures opérationnelles d'exploitation (systèmes, applications, équipements et solutions réseau et sécurité, etc.), • Interview du DSI, du RSI et des différents administrateurs (système, réseau, BD, ...), • Interview d'un échantillon d'utilisateurs supposés utiliser ces procédures, • vérification du rapport d'audit de l'authenticité et la pertinence des procédures opérationnelles.	• Procédures opérationnelles d'exploitation, • Historique des MAJ des procédures opérationnelles, • Rapports d'audit de l'authenticité et la pertinence des procédures opérationnelles.
A.12.1.4	Séparation des environnements de développement, de test et d'exploitation	Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.	• Si les environnements de développement et de test sont séparés des environnements opérationnels, • Si les serveurs applicatifs (où sont installées les applications) et BD s'agissent des serveurs dédiés.	• Interview de l'administrateur système et d'un échantillon de développeurs et testeurs, • Vérification sur les serveurs.	• Inventaire des serveurs de l'environnement opérationnel, • Inventaire des serveurs de développement et de test.

Contenu

A.13	**Sécurité des communications**				
A.13.1	Gestion de la sécurité des réseaux	Objectif: Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.			
A.13.1.1	Contrôle des réseaux	Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.	• Si les responsabilités et les procédures de gestion des équipements réseau sont définies, • Si la responsabilité d'exploitation des réseaux est séparée de celle de l'exploitation des ordinateurs, • Si des mesures spéciales pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics ou les réseaux sans fil sont mises en place, • Si des mesures spéciales pour maintenir la disponibilité des services réseau sont mises en place, • Si les actions susceptibles d'affecter la sécurité de l'information sont détectées et journalisées, • Si les systèmes sont authentifiés sur le réseau.	• Revue de la procédure de gestion des équipements réseau, • Revue des fiches de postes des administrateurs réseau, • Revue du schéma synoptique de l'architecture du réseau, • Revue du diagramme des flux réseau, • Revue de l'inventaire des équipements réseau et de sécurité, • Interview des administrateurs réseau, • Audit des comptes d'administration des équipements réseaux et de sécurité (compte partagé par tous les admins ou comptes nominatifs), • Audit des configurations de ces équipements, • Revue des ACLs sur ces équipements, • Revue des logs de ces équipements et identification des actions éventuelles pouvant avoir un impact sur la sécurité des réseaux (ex : accès par des outils non sécurisé tel que Telnet).	• Procédure de gestion des équipements réseau, • Fiches de postes des administrateurs réseau, • Schéma synoptique de l'architecture du réseau, • Diagramme des flux réseau, • Inventaire des équipements réseau et de sécurité, • Rapport d'audit des comptes d'administration des équipements réseaux et de sécurité, • Fichiers de configuration et ACL des équipements réseau et de sécurité, • Logs de ces équipements.
A.13.1.2	Sécurité des services de réseau	Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans	• Si la capacité du fournisseur de services de réseau à gérer ses services de façon sécurisée est déterminée et surveillée régulièrement, • Si un accord sur le droit à	• Revue des accords de niveau de service (SLA) conclus avec les fournisseurs de service internes ou externes, • Revue de l'accord sur le droit à auditer,	• Accords de niveau de service (SLA) conclus avec les fournisseurs de service internes ou externes, • Accord sur le droit à

Contenu

A.14	**Acquisition, développement et maintenance des systèmes d'information**				
A.14.1	Exigences de sécurité applicables aux systèmes d'information	Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d'information fournissant des services sur les réseaux publics.			
A.14.1.1	Analyse et spécification des exigences de sécurité de l'information	Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.	• Si une analyse des risques de sécurité de l'information est réalisée dès la phase de conception des nouveaux systèmes d'information ou leur amélioration, • Si le niveau de confiance requis en ce qui concerne l'identité déclarée des utilisateurs est pris en compte afin d'en déduire les exigences d'authentification utilisateur.	• Revu du document d'analyse des risques, • Revue des documents de projets de développement de nouveaux systèmes, • Revue des cahiers des charges pour l'acquisition de nouveaux systèmes, • Revue des contrats avec les fournisseurs, • Revue des critères d'acceptation des produits,	• Document d'analyse des risques, • Documents de projets de développement de nouveaux systèmes, • Cahiers des charges pour l'acquisition de nouveaux systèmes, • Contrats avec les fournisseurs, • Critères d'acceptation
A.14.1.3	Protection des transactions liées aux services d'application	Les informations impliquées dans les transactions liées aux services d'application doivent être protégées pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.	• Si la signature électronique est utilisée par chacune des parties impliquées dans la transaction, • Si le canal de communication entre toutes les parties impliquées est chiffré, • Si les protocoles utilisés, pour la communication entre les parties, sont sécurisés, • Si le stockage des détails de la transaction est situé hors de tout environnement accessible au public, à l'instar d'une plateforme de stockage en place sur l'intranet de l'organisme, et s'il n'est pas conservé ou exposé sur un support de stockage directement accessible depuis Internet, • Si, lorsqu'une autorité de confiance est utilisée (par exemple dans le but d'émettre et de tenir à jour des signatures ou	• Interview des responsables métier et du RSI, • Vérification de l'utilisation de protocoles sécurisés sur les serveurs (ex : certificats SSL), • Vérification des moyens de stockage des détails des transactions, • Vérification du processus de gestion du cycle de vie des certificats électroniques.	• Moyens de stockage des détails des transactions, • Document du processus de gestion du cycle de vie des certificats électroniques.

Contenu

A.15	**Relations avec les fournisseurs**				
A.15.1	Sécurité dans les relations avec les fournisseurs	Garantir la protection des actifs de l'organisme accessible aux fournisseurs.			
A.15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisme doivent être acceptées par le fournisseur et documentées.	• Si une politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'audité est élaborée et mise en œuvre, • Si les types de fournisseurs, (par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique), auxquels l'organisme accordera un accès à son information sont identifiés et documentés, • Si on impose contractuellement à tout fournisseur pouvant avoir accès ou favoriser l'accès à des informations ou à des ressources sensibles, que ses collaborateurs signent un engagement personnel de respect des clauses de sécurité spécifiées, • Si une analyse des risques liés aux accès du personnel du fournisseur au système d'information ou aux locaux contenant de l'information est réalisée et si les mesures de sécurité nécessaires sont définies en conséquence, • Si les types d'accès à l'information que les différents types de fournisseurs se verront accorder sont définis et si ces accès sont surveillés et contrôlés, • Si les incidents et les impondérables associés aux accès fournisseurs, incluant les responsabilités de l'organisme et celles des fournisseurs sont identifiés et traités.	• Revue de la politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'audité, • Revue de la liste des types de fournisseurs, (par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique), • Revue des engagements personnels de respect des clauses de sécurité signés par les collaborateurs du fournisseur, • Revue du rapport d'analyse des risques liés aux accès du personnel du fournisseur, • Revue de la définition des types d'accès à l'information accordés aux différents types de fournisseurs, • Revue du rapport de traitement des incidents et des impondérables associés aux accès fournisseurs	• Politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'audité, • Liste des types de fournisseurs, (par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique), • Engagements personnels de respect des clauses de sécurité signés par les collaborateurs du fournisseur • Rapport d'analyse des risques liés aux accès du personnel du fournisseur, • Liste des types d'accès à l'information accordés aux différents types de fournisseurs, • Rapport de traitement des incidents et des impondérables associés aux accès fournisseurs.

Contenu

A.16	Gestion des incidents liés à la sécurité de l'information				
A.16.1	Gestion des incidents liés à la sécurité de l'information et améliorations	Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.			
A.16.1.1	Responsabilités et procédures	Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.	• Si des responsabilités pour garantir une gestion efficace des incidents sont définies et documentées, • Si les procédures suivantes sont élaborées et mises en œuvre : - procédure de surveillance, de détection, d'analyse et de signalement des événements et des incidents liés à la sécurité de l'information, - procédure de journalisation des activités de gestion des incidents, - procédure de traitement des incidents,	• Revue du document de définition des responsabilités relatives à la gestion des incidents, • Revue des fiches de postes du personnel affecté à la gestion des incidents, • Revue des différentes procédures de gestion des incidents, • Revue d'un échantillon de fiches d'incidents, • Interview du DSI et du RSI.	• Document de définition des responsabilités relatives à la gestion des incidents, • Fiches de postes du personnel affecté à la gestion des incidents, • Procédures de gestion des incidents, • Echantillon de fiches d'incidents.
A.16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision	Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information.	• Si les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites sont analysés, • Si les applications et les systèmes sensibles disposent d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des stations voisines ou tentatives infructueuses de transactions sensibles, tentatives	• Revue du rapport d'analyse des événements liés à la sécurité de l'information, • Revue de l'archive de tous les éléments de diagnostic, • Revue des enregistrements de l'analyse des événements et des conclusions prises, • Interview du DSI et du RSI, • Audit de la configuration des serveurs, des BD et des équipements réseau et de sécurité, • Audit de la configuration du système de détection d'intrusion, • Revue des logs des accès sur les serveurs, les BD et les équipements	• Rapport d'analyse des événements liés à la sécurité de l'information, • Archive de tous les éléments de diagnostic, • Enregistrements de l'analyse des événements et des conclusions prises, • Rapport d'audit de la configuration des serveurs, des BD et des équipements réseau et de sécurité, • Fichier de configuration du système de détection d'intrusion,

Contenu

A.17	**Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité**				
A.17.1	Continuité de la sécurité de l'information	La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité.			
A.17.1.1	Organisation de la continuité de la sécurité de l'information	L'organisme doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management	• Si une analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information est réalisée,	• Revue du rapport d'analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information, • Revue du document des exigences	• Rapport d'analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information,
		de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre	• Si les exigences de sécurité de l'information applicables aux situations défavorables sont déterminées, à la lumière des résultats de l'analyse de l'impact, et documentées, • Si les objectifs de continuité de la sécurité de l'information sont approuvés par la direction, • si la continuité de la sécurité de l'information est intégrée au processus de gestion de la continuité de l'activité ou au processus de gestion de la récupération après sinistre, • Si les exigences de continuité de la sécurité de l'information sont formulées de manière explicite dans les processus de gestion de la continuité de l'activité et de gestion de la récupération après sinistre.	de sécurité de l'information applicables aux situations défavorables, • Revue du processus de gestion de la continuité de l'activité et de gestion de la récupération après sinistre, • Interview du DSI et du RSI.	• Document des exigences de sécurité de l'information applicables aux situations défavorables, • Processus de gestion de la continuité de l'activité et de gestion de la récupération après sinistre.
A.17.2	Redondances	Garantir la disponibilité des moyens de traitement de l'information			
A.17.2.1	Disponibilité des moyens de traitement de l'information	Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.	• Si une solution de secours (systèmes redondants) est mise en place pour pallier l'indisponibilité de tout équipement ou de toute liaison critique, • Si cette solution de secours est parfaitement opérationnelle, • Si la capacité de cette solution de secours assure une charge opérationnelle suffisante et est approuvée par les utilisateurs,	• Revue de l'inventaire du matériel, • Revue des rapports de tests de la solution de secours, • Interview du DSI et du RSI.	• Inventaire du matériel, • Rapports de tests de la solution de secours.

Contenu

A.18	Conformité				
A.18.1	Conformité aux obligations légales et réglementaires	Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.			
A.18.1.1	Identification de la législation et des exigences contractuelles applicables	Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisme pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisme elle-même.	• Si l'ensemble des exigences réglementaires, contractuelles, et légales applicable à l'audité sont explicitement identifiées, documentées et tenues à jour, • Si les mesures spécifiques et les responsabilités individuelles mises en place sont définies et documentées pour répondre à ces exigences.	• Revue des documents relatifs aux exigences réglementaires, contractuelles, et légales, • Revue du document des mesures spécifiques et des responsabilités individuelles mises en place pour répondre à ces exigences, • Interview du DSI, du RSI, du responsable juridique et du DRH.	• Documents relatifs aux exigences réglementaires, contractuelles, et légales, • Historique des MAJ de document, • Document des mesures spécifiques et des responsabilités individuelles mises en place pour répondre à ces exigences.
A.18.1.2	Droits de propriété intellectuelle	Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et	• Si une procédure est élaborée et mise en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à	• Revue de la procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels	• Procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle
A.18.1.3	Protection des enregistrements	Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.	• Si une procédure de stockage et de manipulation des enregistrements est élaborée et mise en œuvre, • Si des mesures de protection des enregistrements sont mises en place conformément à leur classification telle que définie par le plan de classification de l'audité, • Si le système de stockage et de manipulation des enregistrements garantit l'identification des enregistrements et de leur durée de conservation telles que définies par la législation nationale ou par les réglementations en vigueur.	• Revue de la procédure de stockage et de manipulation des enregistrements, • Interview du DAF, DRH DSI et RSI, • Audit des droits d'accès aux enregistrements au niveau des bases de données.	• procédure de stockage et de manipulation des enregistrements, • rapport d'audit des droits d'accès aux enregistrements.